Can cyber insurance combat cyber crime?

In a world where so much information is stored digitally, cyber attacks that hold computers hostage can be incredibly damaging. **Dr Jason Nurse**, from the Institute of Cyber Security for Society at the **University of Kent**, UK, and **Jamie MacColl**, from the UK's **Royal United Services Institute**, are investigating whether companies can use cyber insurance to help mitigate the threat from cyber criminals.

Dr Jason R.C. Nurse

Institute of Cyber Security for Society (iCSS) and School of Computing, University of Kent, UK

Jamie MacColl

Royal United Services Institute (RUSI), UK

PROFILES

Field of research
Cyber Security

Research project
Investigating the effectiveness of cyber insurance against ransomware attacks

Team members
Gareth Mott, Sarah Turner, James Sullivan, Pia Huesch, Anna Cartwright and Edward Cartwright

Funder
UK National Cyber Security Centre (NCSC)

TALK LIKE A ...

CYBER SECURITY EXPERT

Cyber attack — an attack against a computer system

Cyber security — protecting computer systems and networks from cyber attacks

Insurance — when a provider agrees to compensate an individual or organisation for a future loss, in return for a regular payment. With cyber insurance, a provider agrees to compensate an individual or organisation if they suffer a cyber attack

Malware — software designed to perform an unauthorised action that will impact the security of a computer system

Policy — a set of guidelines

Policymaker — someone who creates policies

Ransomware — malware that blocks access to a computer system until a ransom is paid

Stakeholder — a person with an interest (a 'stake') in a particular topic

Think tank — a group of experts on a particular topic that engage with researchers and policymakers to provide policy advice

In the 17th century, pirates would kidnap wealthy merchants and demand money in exchange for their safe release. Today, the ransoming of digital data by cyber criminals is far more likely. Cyber security researchers Dr Jason Nurse, from the University of Kent's Institute of Cyber Security for Society (iCSS), and Jamie MacColl, from the Royal United Services Institute (RUSI), have teamed up to analyse the impacts of ransomware, investigate whether cyber insurance can protect organisations from these attacks, and influence national cyber security policies.

What are the impacts of ransomware?

"Ransomware is a form of cyber attack," explains Jason. "A cyber criminal installs malware on a computer system, which blocks access to the computer and all the data contained on it. The criminal then demands money and only removes the malware once the computer owner has paid the ransom." As today's world is driven by technology, if organisations lose access to computer files or networks it can have disastrous impacts.

Beyond the cost of the ransom demand (which can range from hundreds to millions of pounds), there are additional factors that make the cost of a ransomware attack much greater. "The company will lose money during the time it can't access the computer network," says Jason. "There will also be damage to the company's reputation, negative impacts on individuals' well-being, and potential harm to wider society." For example, a ransomware attack on the UK's National Health Service (NHS) in 2017 had huge knock-on impacts as hospitals were unable to access patients' medical records, which meant doctors could not carry out medical procedures.

"Educational institutions are increasingly being hit by ransomware attacks," says Jason. "They hold a huge amount of sensitive data about

students and, unfortunately, their cyber security is often not very strong, so criminals see them as a good target." In 2022, several UK schools were attacked, with the hackers leaking highly confidential documents containing children's data online.

Cyber criminals do not only target organisations, they also attack individuals. Your phone contains a wealth of information about you that hackers would love to get hold of. Not only could a ransomware attack result in you losing access to your phone and accounts, but criminals could also steal your data (and that of all your contacts) and sell or share it online.

What are the challenges of researching ransomware attacks?

Jason, Jamie and their team are investigating the nature and impacts of ransomware attacks, in the hope of informing public policies that will help protect organisations. However, this is not always an easy task. "There are three main challenges to analysing ransomware: underreporting, long-term impacts and non-financial costs," says Jason.

Underreporting happens because many ransomware incidents are never revealed by the companies affected. "To avoid bad publicity, many companies quietly pay off the criminals and struggle to recover by themselves, without ever reporting the attack," says Jamie. "If we don't learn of these incidents, we don't learn from them either." Even when attacks are reported, the long-term impacts are difficult to measure. Impacts can continue for months as the organisation recovers, so it is hard to quantify the total cost of the incident. Non-financial costs are also difficult to measure, especially the impact on people's psychological well-being. "How do you put a number on the level of stress faced by a teenager who knows their personal details have been shared online, a doctor who can't help their patients or an IT professional working long shifts to recover a company's computer systems?" asks Jason.

Can cyber insurance protect against ransomware attacks?

If you have phone insurance, you pay a small amount of money every month to an insurance provider and, in return, they will pay to repair your phone if it breaks. Cyber insurance works in the same way: organisations pay a regular fee to an insurance provider, who will cover the cost of the ransom, should the organisation be attacked by cyber threats such as ransomware.

> **"IT'S IMPORTANT TO BRING IN DIFFERENT PERSPECTIVES FROM DIFFERENT AREAS OF EXPERTISE SO WE CAN FIND THE BEST SOLUTIONS TO THE CHALLENGE."**

Jason and Jamie work with people involved in all aspects of preventing and responding to ransomware attacks, including insurance providers, cyber security experts and companies who have been attacked. "We hold workshops that bring these stakeholders together, to learn how ransomware is impacting organisations and how insurance can help to reduce this threat," says Jamie. "It's important to bring in different perspectives from different areas of expertise so we can find the best solutions to the challenge."

So far, the team has discovered that the process of applying for cyber insurance encourages companies to improve their cyber security. "The cost of insurance depends on the likelihood that the provider will need to pay out in the future," says Jason. "For instance, your home insurance will be cheaper if you have good locks on your doors and windows and live in an area with low crime, because your provider knows it's less likely that you will be burgled." It is the same concept for cyber insurance: if a company has good cyber security, they are less likely to suffer a ransomware attack, so their cyber insurance will be cheaper. "We have discovered that companies improve their cyber security before applying for cyber insurance, as this reduces the cost of insurance," says Jamie. "In this way, cyber insurance has a positive impact on cyber security."

However, the overall effect of cyber insurance on cyber security is less clear when criminals' motives are also considered. "There is anecdotal evidence that cyber criminals deliberately target companies that have cyber insurance, because they know the ransom will be paid by the insurance provider," says Jason. In the same way that ancient pirates attacked wealthy merchant ships rather than poor fishing boats as there was a greater chance of the ransom being paid, modern cyber criminals attack organisations that are more likely to pay up. "This means that, when all factors are considered, it's hard to know whether cyber insurance has a positive or negative effect on cyber security."

How can this academic research influence policy?

The collaboration between iCSS (an academic research institute) and RUSI (a government think tank) is key to Jason and Jamie's project, as it ensures the research findings are used effectively to improve society. "Our relationship allows us to produce robust research that addresses significant societal issues and communicate our policy recommendations directly with policymakers," explains Jason.

Not only does Jamie contribute to the team's research, but in his role at RUSI he is also responsible for communicating the project's findings with the government and wider public, by engaging with the UK Parliament and the media. "I recently presented the results of our ransomware research to members of a UK Parliamentary Committee, to help them understand the issues around cyber security and ransomware," he says. "In this way, our research is influencing important policy decisions around cyber security at a national level."

About *cyber security*

Ever since computers entered mainstream use, criminals have been attacking them. "Today, a ransomware attack happens every 14 seconds!" says Jamie. As society relies so heavily on computers and digital information, protecting them from cyber attacks is a vital task. Cyber security does not just depend on the computer scientists and software engineers who design the technical solutions to protect computers; it also requires an understanding of human behaviour.

"It is important to apply theories and approaches from psychology to better understand and find solutions for cyber security problems," explains Jason. "By working with psychologists, we can learn why people make the decisions they do (such as opening unknown files or clicking on dodgy links) and use this knowledge to help make policy recommendations."

Cyber security is a constant 'arms race' between security systems and cyber criminals, as each side develops more sophisticated software to outwit their opponents. "Artificial intelligence (AI) will inevitably provide the next challenge and opportunity for both sides," says Jason. "While cyber security experts can use AI to detect and defend against cyber attacks, cyber criminals can use it to scale up their attacks. I've already seen ChatGPT used to launch cyber attacks."

To inform the future of cyber security, Jamie recommends learning from past experiences. "There is an ongoing lack of awareness and investment in cyber security," he says. "Many of the current challenges we face are new versions of old cyber security problems, so understanding the future requires studying the past."

Jason and Jamie's tips *for staying safe online*

- Be careful what you share online. Even if later removed, anything posted online is potentially accessible forever, and criminals can harvest it for information.
- Check the privacy settings of your devices, applications and social media accounts. Who can see what you post online? What information are technology companies collecting about you?
- Protect all your accounts with strong, distinct passwords. Using a password manager is helpful for this.
- Use two-factor authentication to add additional protection to your accounts and devices, by requiring two forms of identification to access them.

Pathway from school to *cyber security*

- Computer science, information technology (IT), software engineering and maths are very useful subjects for a technical career in cyber security.
- There is also a range of non-technical careers in cyber security that rely on people with backgrounds in psychology, politics, international relations and public policy, so studying any of these could also lead to a career in the field.
- You can gain practical hands-on experience in cyber security while at school through programmes such as Hack the Box (**www.hackthebox.com**), where you can learn how to identify weaknesses in computer systems by penetration testing (also known as 'ethical hacking').
- The CyberFirst programme (**www.ncsc.gov.uk/cyberfirst**) run by the National Cyber Security Centre (NCSC) has a range of activities, resources, courses and competitions to help you stay safe online and inspire you to consider a career in cyber security.
- The NCSC also offers bursaries and apprenticeships to support students hoping to pursue a career in cyber security: **www.ncsc.gov.uk/cyberfirst/bursary-and-degree-apprenticeship**

Explore careers in *cyber security*

- "So much of today's world is built on technology, and this technology needs to be secured," says Jason. "This means there is an ever-increasing range of career opportunities in cyber security."
- Technical careers in cyber security include systems and security architects (who build secure computer systems), penetration testers (who try to ethically hack into computer systems to test a network's defences) and IT security managers (who oversee an organisation's digital systems).
- You do not need a technical computer background to have a career in cyber security. The human component of cyber security means that, with a background in behavioural psychology, you could work to understand how and why people make decisions that harm computer systems. Or, if you are interested in geopolitics, you could work in cyber threat intelligence. Governments and think tanks also need people interested in the intersection of cyber security and public policy to create policies that protect organisations from cyber attacks.
- Prospects provides information about careers in cyber security, including the qualifications you may need and the salary you can expect: **www.prospects.ac.uk/job-profiles/cyber-security-analyst**

Meet *Jason*

I've always been interested in computers and technology. Who would've thought that one day we would be able to find the answer to any question on our phone, or take phone calls from our watch? Technological progress is fascinating!

It's important to know that you don't have to be great with computers and technology to work in cyber security. I studied maths, accounting and business studies at school, then accounting and computer science at university. After graduating, I worked as an auditor, and it was only later that I realised I wanted a career in cyber security.

I am inspired by the reality that my work makes the world a safer place. Cyber attacks are constantly evolving, so cyber security must always be one step ahead. This means I'm constantly addressing new challenges, and it's exciting to work in a field that's so dynamic.

Alongside conducting academic research, I also work in industry. I'm the director of science and research at a cyber security company, where I lead a team of scientists conducting innovative work to inform the company's products. Although we produce technology outputs, most of the researchers are psychologists, highlighting the importance of understanding human behaviour for addressing cyber security challenges. It's great to have a practical application for my research and to know that I'm helping to ensure that computer systems are built in a robust and evidence-based way.

Jason's *top tip*

Find a good mentor. It is important to have people you can look up to and who can guide you through your studies and career.

Meet *Jamie*

I have a bachelor's degree in war studies and a master's in international relations and politics, which might not seem like an obvious route to a career in cyber security. However, these subjects link to geopolitics and, as it's important to understand nations' motives when preparing for global cyber threats, many of my classmates now also work in the field, particularly in cyber threat intelligence.

While at university, I did an internship at a small cyber threat intelligence company. The experience was hugely valuable as I learnt practical skills, such as writing daily intelligence reports, and I contributed to genuine research projects. Wherever possible, I highly recommend that students seek out meaningful internships.

I enjoy conducting research interviews with experts from government and industry and bringing these people together through workshops to learn from their experiences. In addition, I like the intellectual exercise of figuring out complex policy challenges.

Music is my passion and has always been an important part of my life. I have been in a band, the Bombay Bicycle Club, since I was 14. We still play together, touring and performing as professional musicians. Playing live music on stage is the best feeling ever! Having two careers keeps me very busy, and while they are completely unrelated, my experiences as a young musician taught me how to communicate with the media – a valuable skill that helps me in my current role as I educate the public about cyber security research.

Jamie's *top tip*

You don't need to have everything figured out when you're 18 – or even when you're 30! Instead, be open to any experience that comes your way and accept that life might not follow the path you expect.

Technology is everywhere in our lives © Joe Edmunds